**11 клас**

**Тема уроку «Політика безпеки при доступі до мережі загального користування.** **Системи аналізу вмісту поштового і веб-трафіку (електронна пошта і НТТР). Віртуальні приватні мережі (VPN). Практична робота №3 «Створення віртуальних приватних мереж»»**

**Практична частина:**

1.Законспектувати наступне:

Існує два підходи до проблеми забезпечення безпеки комп'ютерних систем (КС) та мереж: «частковий» і комплексний.

«Частковий» підхід спрямований на протидію чітко визначеним загрозам у заданих умовах. Перевагою такого підходу є висока вибірковість до конкретної загрози. Істотний недолік - відсутність єдиної захищеної середовища обробки інформації.

Комплексний підхід орієнтований на створення захищеного середовища обробки інформації в КС, що об'єднує в єдиний комплекс різнорідні заходи протидії загрозам. Організація захищеного середовища обробки інформації дозволяє гарантувати певний рівень безпеки КС, що є перевагою комплексного підходу. До недоліків цього підходу відносяться: обмеження на свободу дій користувачів КС, чутливість до помилок установки і налаштування засобів захисту, складність управління.

**Система mail-контент.**

Система являє собою набір політик, правил, фільтрів для аналізу вхідного і вихідного поштового трафіку.

Існує два способи роботи системи:

«В розриві»;

«В відгалуженні»

У «розриві» - це режим, при якому вся вхідна та вихідна кореспонденція обов'язково проходить крізь контент - систему, яка, працюючи в online режимі, здійснює аналіз пошти і приймає рішення: відправка / затримка ітд.

У «відгалуженні» - це режим, при якому система отримує копію поштового потоку. Аналіз вмісту і реакція на порушення політик йде як постфактум.

Система mail-контент складається з двох груп серверів:

-розбору поштового потоку;

-зберігання поштових повідомлень.

**Система web - контент.**

Система являє собою набір політик, правил роботи, фільтрів. На відміну від mail - контенту, web - контент може бути встановлений тільки в розрив. Система також складається з двох груп серверів:

-аналіз вмісту web - трафіку (а так само кешування потоку);

-зберігання журналів (логів і звітів).

Віртуальна приватна мережа (VPN) створюється на базі загальнодоступної мережі Інтернет.

Технологія VPN створює віртуальні канали зв’язку через загальнодоступні мережі, так звані «VPN—тунелі». Трафік, що проходить через тунелі, що зв’язують віддалені філії, шифрується.

Загрози, пов'язані з використанням VPN:

-недостатній рівень захисту даних забезпечується власниками VPN сервісами/

-безкоштовні сервіси є менш захищеними ніж платні.

-можливість крадіжки особистих даних.

-передача даних невідомим адресатам.

2) Виконайте практичну роботу №3:

1.Відкрийте Налаштування.

2.Натисніть Мережа й Інтернет Потім Додатково Потім VPN.

3.Угорі праворуч натисніть значок Додати.

4.Введіть дані.

5.Натисніть Зберегти.

**Домашнє завдання:**

1. Опрацювати теоретичний матеріал по темі.

Результат відправити на e-mail: [**firstschool1227@gmail.com**](mailto:firstschool1227@gmail.com). (в темі вказати прізвище, предмет та клас).

**Тема уроку «Антивірусні засоби захисту. Загальні правила застосування антивірусних засобів в автоматизованих системах»**

**Практична частина:**

1.Законспектувати наступне:

**Комп'ютерний вірус** – це програмне забезпечення, метою якого є проникнення на комп'ютер користувача, створення своїх копій і приховане виконання шкідливих дій.

Характерні дії вірусу:

-знищення даних шляхом видалення файлів певних типів або фор­матування дисків;

-внесення змін у файли, зміна структури розміщення файлів на диску;

-зміна або повне видалення даних із постійної пам’яті;

-зниження швидкодії комп’ютера;

-постійне розміщення в оперативній пам’яті і ураження нових об’єктів;

-примусове перезавантаження операційної системи;

-блокування запуску певних програм;

-збирання і пересилання копії даних комп’ютерними мережами;

-використання ресурсів уражених комп’ютерів для організації ко­лективних атак на інші комп’ютери в мережах;

-виведення звукових або текстових повідомлень, спотворення зобра­ження на екрані монітора тощо.

Види вірусів:

безпечні - проявляються відео та звуковими ефектами, не змінюють фай­лову систему, не ушкоджують файли і не виконують шпигунські дії;

небезпечні - призводять до перебоїв у роботі комп’ютерної системи: зменшують розмір доступної оперативної пам’яті, перезавантажують комп’ютер тощо;

дуже небезпечні - знищують дані з постійної та зовнішньої пам’яті, виконують шпигунські дії тощо.

Принципи розповсюдження вірусів:

-дискові (завантажувальні) віруси - розмножуються копіюванням себе в службові ділянки дисків та інших змінних носіїв, яке відбу­вається під час спроби користувача зчитати дані з ураженого носія;

-файлові віруси - розміщують свої копії у складі файлів різного ти­пу. Як правило, це файли готових до виконання програм із розши­ренням імені ехе або сот.

-хробаки (черв’яки) - пересилають свої копії комп’ютерними мережами з метою проникнення на віддалені комп’ю­тери. Більшість черв’яків поширюються, прикріпившись до файлів електронної пошти, електронних документів тощо.

-троянські програми - програми, що проникають на комп’ютери ко­ристувачів разом з іншими програмами, які користувач «отримує в дарунок» комп’ютерними мережами.

Антивірус - це комплекс програм, призначений для виявлення і знешкодження шкідливого програмного забезпечення, а також для усунення наслідків його дій.

Функції антивірусного програмного забезпечення:

-Моніторинг файлів.

-Перевірка файлів на зараження з метою, локалізації та подальшого лікування.

-Своєчасне оновлення антивірусних баз даних.

**Домашнє завдання:**

1. Опрацювати теоретичний матеріал по темі.
2. Результат відправити на e-mail: [**firstschool1227@gmail.com**](mailto:firstschool1227@gmail.com). (в темі вказати прізвище, предмет та клас).